



HI-TECH CRIME TRENDS 2018

group-ib.com



HARDWARE VULNERABILITIES AND BIOS/UEFI SECURITY

HARDWARE VULNERABILITIES

MELTDOWN AND SPECTRE

JANUARY 2018

- Variant 1: Bounds Check Bypass – CVE-2017-5753
- Variant 2: Branch Target Injection – CVE-2017-5715
- Variant 3: Rogue Data Cache Load – CVE-2017-5754
- Variant 3a: Rogue System Register Read – CVE-2018-3640
- Variant 4: Speculative Store Bypass – CVE-2018-3639

GLITCH

MAY 2018

The specialists successfully tested the GLitch technique on an Android device with Chrome and Firefox browsers. They were able to compromise the device in just 2 minutes. To exploit the attack technique, all they had to do was to upload the malicious JavaScript code to the target device.

MELTDOWNPRIME AND SPECTREPRIME

FEBRUARY 2018

SpectrePrime code proposed by researchers as a proof of concept leads to the success of 99.95% of the attacks on an Intel processor (the success rate of the usual attacks by Spectre reaches 97.9%).

TLBLEED

JULY 2018

It was demonstrated that cryptographic keys and other important data can be extracted from another running program with a minimum success rate of 98%. Despite the fact that the vulnerability was not identified with CVE, OpenBSD developers decided not to support Hyper-Threading in Intel processors.

99.95%

success rate when using SpectrePrime

2 MINUTES

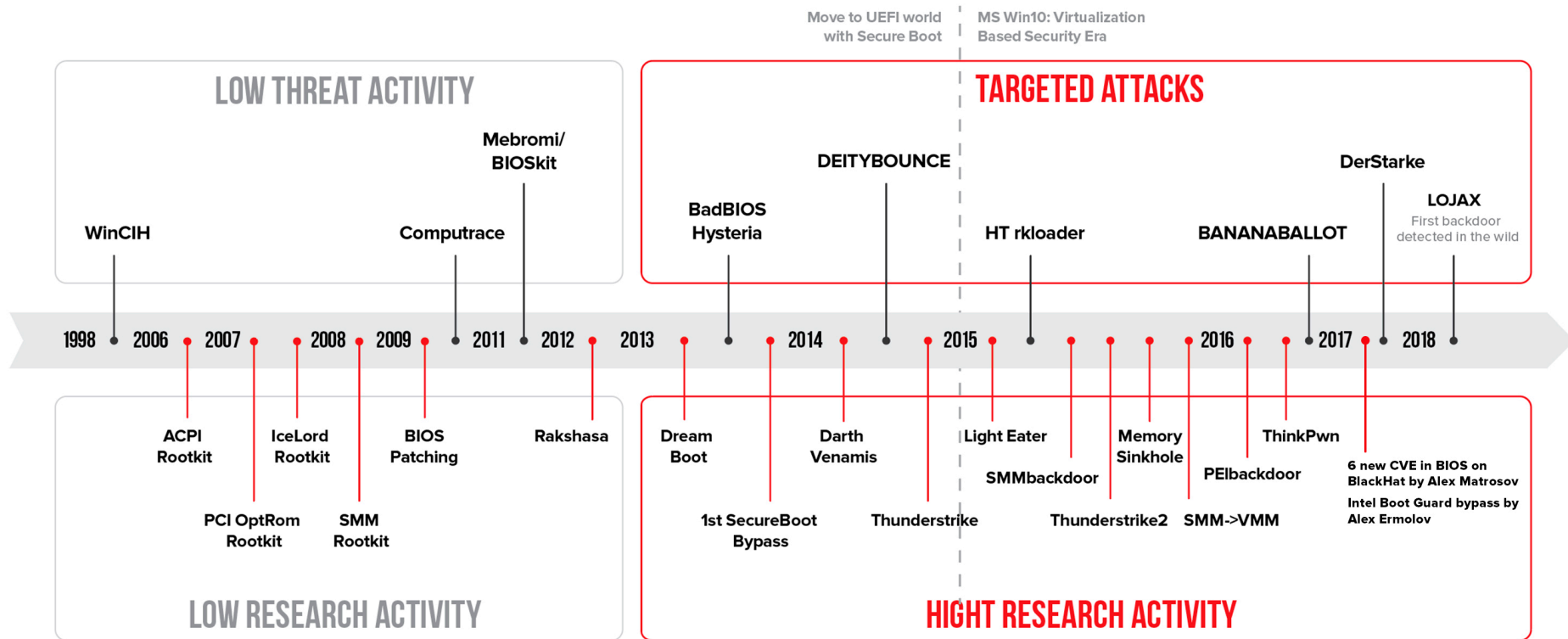
needed to compromise an Android-based device using the GLitch technique

98%

success rate of the attack and cryptographic keys extraction using TLBleed



BIOS/UEFI THREATS





APT, ESPIONAGE IS THE MAIN TASK



HOME DEVICES ARE A NEW TARGET

- Undetectable penetration vector
- Even stealthier method of data collection
- Creates more opportunities to attack other devices in a local network
- Good persistence



30% OF APT GROUPS USE LEGAL FRAMEWORKS

METASPLOIT






- Turla
- Lazarus
- OilRig
- Charming Kitten
- Newscaster Team
- APT32
- MuddyWater

COBALT STRIKE

- APT17
- APT10
- TEMP.Periscope



APT, ESPIONAGE IS THE MAIN TASK

AMERICA 	EUROPE 	APAC 	MIDDLE EAST & AFRICA 	RUSSIA 
<ul style="list-style-type: none">• APT28 Russia• Turla Russia• Lazarus North Korea• APT15 China• Thrip China• Charming Kitten Iran• Mustang Panda China• Dragonfly Russia• Orangeworm• Gorgon Group Pakistan• TEMP.Periscope China• Newscaster Team Iran	<ul style="list-style-type: none">• Lazarus North Korea• APT28 Russia• APT15 China• Tick China• BlackEnergy Russia• Dragonfly Russia• TEMP.Periscope China• Orangeworm• Gorgon Group Pakistan• PowerPool	<ul style="list-style-type: none">• DarkHotel North Korea• Lazarus North Korea• Thrip China• APT32 Vietnam• Mustang Panda China• APT37 North Korea• Slingshot USA• Kimsuky North Korea• Andariel North Korea• Tick China <ul style="list-style-type: none">• BlackEnergy Russia• APT28 Russia• Charming Kitten Iran• Orangeworm• MuddyWater Iran• Sidewinder India• Chafer Iran• APT-C-35• Rancor• TEMP.Periscope China• APT17 China	<ul style="list-style-type: none">• OilRig Iran• APT37 North Korea• Slingshot USA• Newscaster Team Iran• APT34 Iran• APT33 Iran	<ul style="list-style-type: none">• Equation - USA• APT10 - China• APT17 - China• PlugX - China• Prikormka - Ukraine• APT28 - Russia• BlackEnergy - Russia• PowerPool

**OPEN SOURCES ONLY PUBLISH INFORMATION
ON ATTACKS ORIGINATING IN DEVELOPING COUNTRIES**



APT, ESPIONAGE IS THE MAIN TASK

LATE 2017 TO EARLY 2018

FINANCE

- **BlackEnergy** attacks Japanese banks with ONI ransomware.

COVERT TARGETS

- **BadRabbit:** mass attacks to conceal real targets under attack.
- **VPNFilter:** about 500,000 routers in 54 countries were infected. One module was detecting SCADA systems.

POWER ENGINEERING

- **BlackEnergy:** espionage in SCADA systems without impact
- **Triton:** framework for manipulating Safety Instrumented System by Schneider Electric with the real accident.

FEBRUARY 2018

OLYMPICS 2018

- **APT28:** Olympic Destroyer was used to disable the official website of the Olympics and Wi-Fi at the stadium; it also affected live broadcast of the opening ceremony.

JANUARY TO MAY 2018

FINANCE

- **Lazarus** puts 9,000 computers and more than 500 servers out of action after Banco de Chile and Bancomext robbery.

COVER-UP TRANSACTIONS

- Real sabotaging attacks are covered by smoke walls.
- The infrastructure is prepared in advance to create smoke walls.



PREDICTIONS: HARDWARE VULNEARILITIES AND APT THREATS



FIRMWARE AND SIDE-CHANNEL ATTACKS

- They will become the main research vector of APT attackers.
- Current security solutions are not ready for such challenges.



NEXT TARGET OF FIRMWARE THREATS:

- Motherboard manufacturers
- Vendors that supply hardware to state authorities
- Small/new cloud services



FLATS/HOUSES AND PERSONAL DEVICES

- New priority when protecting secrets and business.
- In the private and public sectors these networks lack due attention.

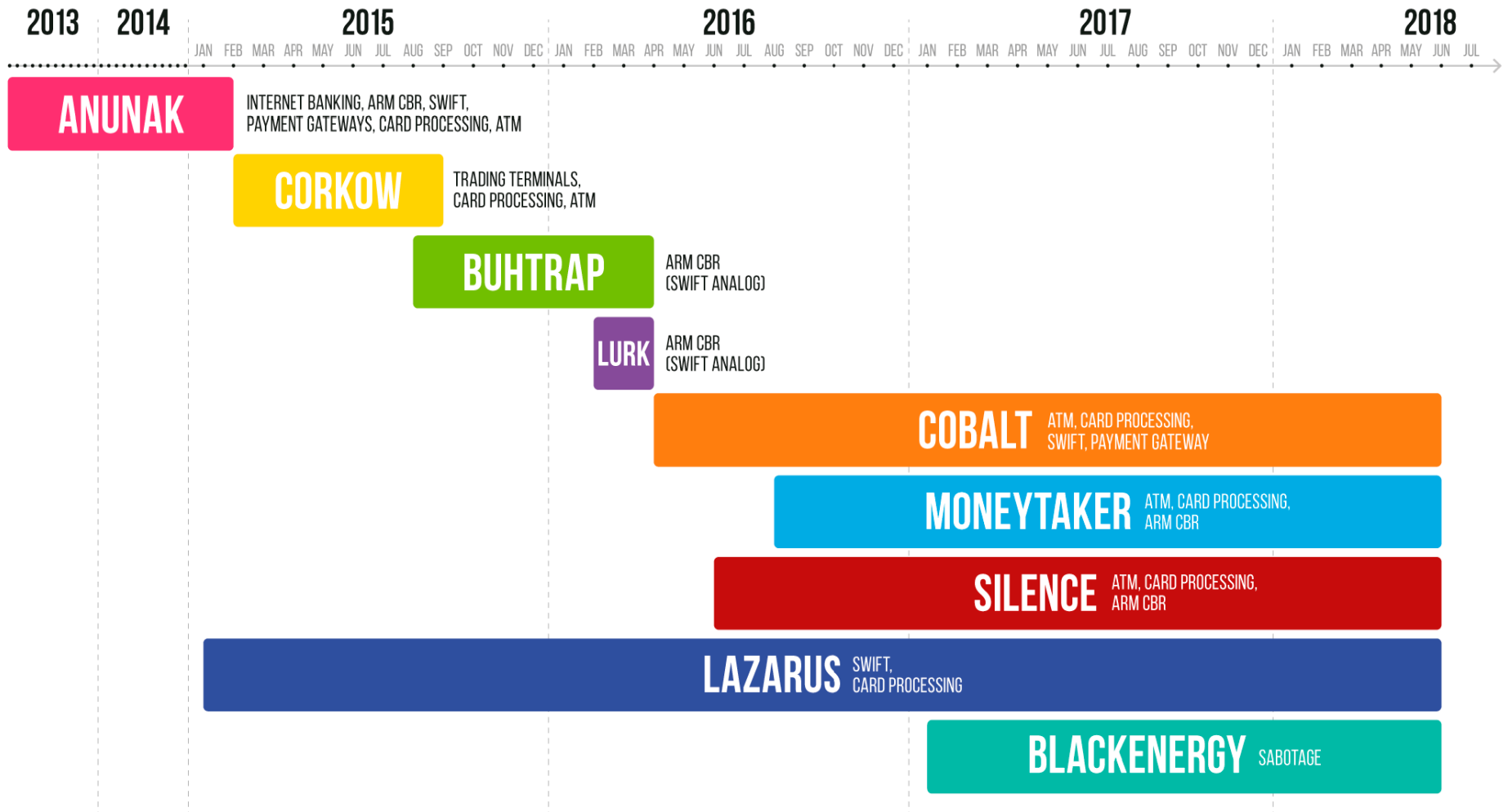


CRITICAL INFRASTRUCTURE

- Initial penetration through vulnerable network hardware, not phishing.
- Self-replicating ransomware will be used to attack air-gapped networks.



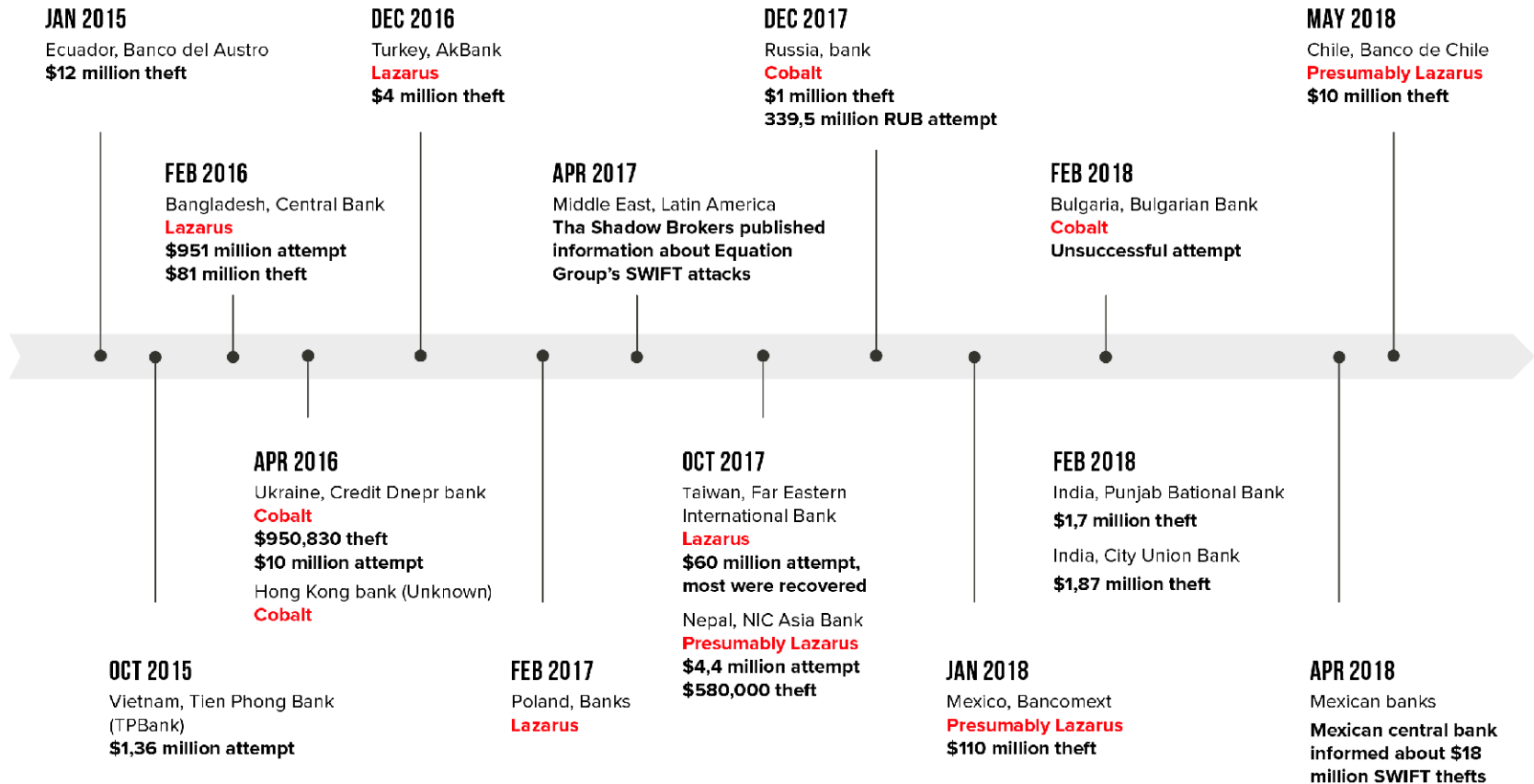
ATTACKS TARGETED AT BANKS



TRADITIONALLY, THE THREAT FOR THE FINANCIAL SECTOR COMES FROM RUSSIAN-SPEAKING ATTACKERS.



ATTACKS TARGETED AT BANKS: INTERBANK SYSTEMS



SWIFT

2 groups are the threat to SWIFT: Lazarus and Cobalt

3 times more incidents

\$26 mln is the average volume of a theft attempt

LOCAL INTERBANK SYSTEMS

They are also targets, but there is no data on the attacks

ARM CBR was attacked only once by MoneyTaker



ATTACKS TARGETED AT BANKS: INTERBANK SYSTEMS



ATTACKS ON ATMS

They draw attackers' attention again. Two groups: MoneyTaker and Silence have created new Trojans for this purpose.



CARD PROCESSING

This is still the main way to monetize access to the banking network in all groups.

Lazarus started using this theft method.



PAYMENT GATEWAYS

This theft method is only used by the Cobalt group.

There were no new attempts after the 2017 attacks.



RUSSIA IS NOT A PRIORITY ANYMORE

All Russian-speaking groups started with attacks in Russia.

Attacks in Russia are not the priority anymore, and all groups attack foreign banks.



PREDICTIONS: ATTACKS TARGETED AT BANKS



ATTACKS OUTSIDE RUSSIA

- First and foremost, we should expect a lot of attacks from Silence.
- Local cybercrime groups will start conducting similar attacks. Above all, we expect growth in the APAC Region.



COMBINED THEFT METHODS

- Lazarus should be expected to steal via SWIFT and card processing at the same time.
- Cybercrime groups will steal via ATMs and card processing.
- Using ransomware after attack completion can become a trend.



INITIAL PENETRATION VECTOR IS CHANGING

- Phishing is still the main vector.
- Some groups will start trying to penetrate banks through web vulnerabilities and vulnerable network hardware.



NEW GROUPS

- After the arrests of Cobalt and Fin7 participants, we can expect new criminal groups to appear.
- Toplel and RTM are the most likely ones to form new groups.



PC TROJANS

STAGNANT DEVELOPMENT WORLDWIDE

- Activity and efficiency of banking Trojans fall all over the world.
- Arrest of Neverquest, GozNym, and Andromeda loader authors hit hard.
- Owners of large botnets use them to install ransomware.

LOCAL NATURE

- Each threat became local and affects 3 to 5 countries on average.

AUTOMATIC TRANSFER SYSTEMS (ATS)

- **New:** BackSwap is the only Trojan with new techniques: a developer's console and a bookmarklet.

BANK PC TROJANS LANDSCAPE

RUSSIA	WORLD
RTM	IcedID
Buhtrap2	BackSwap
Toplel	DanaBot
	MnuBot
	Osiris
	Xbot
	Shifu
	Qadars
	Sphinx
	Tinba
	Emotet
	Dridex
	Trickbot
	Gozi (ISFB, Ursnif)
	Quakbot (Qbot)
	TinyNuke (NukeBot)
	Gootkit
	Ramnit
	ZeusVM (KINS)
	Atmos
	Zeus
	Retefe
	Corebot
	UrlZone Banker
	Panda Banker



ANDROID TROJANS

SECURITY BY GOOGLE

- The main reason for restraining Android threats.
- Old Trojan versions do not work on new Android versions.

SLOWDOWN ABROAD

- 5 Trojans—Xbot, Abrvall, Vasya, UfoBot, Reich—are no longer used due to poor support.
- The most active developer, GanjaMan, who created the most popular versions of Trojans, was blocked, and his developments are no longer used.

TROJANS WITH WEB FAKES GLOBALLY

| Easy | Exobot 2.0 | CryEye | Cannabis
| Fmif | AndyBot | Loki v2 | Nero Banker
| Sagawa | Agent.cj • Maza-in • Loki v2
Alien bot • Rello • Red Alert v2

STAGNANT DEVELOPMENT IN RUSSIA

- The owners of the two largest botnets, Cron and Tiny.z, were arrested
- Honli botnet was disabled.
- Number of thefts became three times smaller, and damage decreased by 77%.
- Average amount of damage was reduced from 11 to 7 thousand.



ATM THREATS

ATM JACKPOTTING

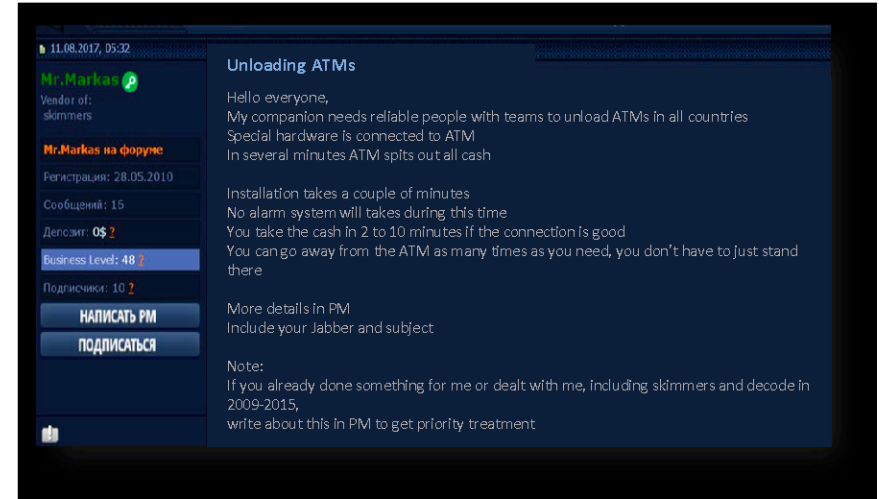
- “New” ATM threat.
- Attackers get physical access to an ATM.
- They plug a microcomputer of a smartphone into the USB/COM port of a dispenser.

CUTLET MAKER

- The main reason for the increase in theft using this method.
- The software is provided in one package with the detailed instruction and an Android app.
- Hacker versions surfaced and led to wider distribution.

MR. MARKAS

- The main software developer for ATM Jackpotting.



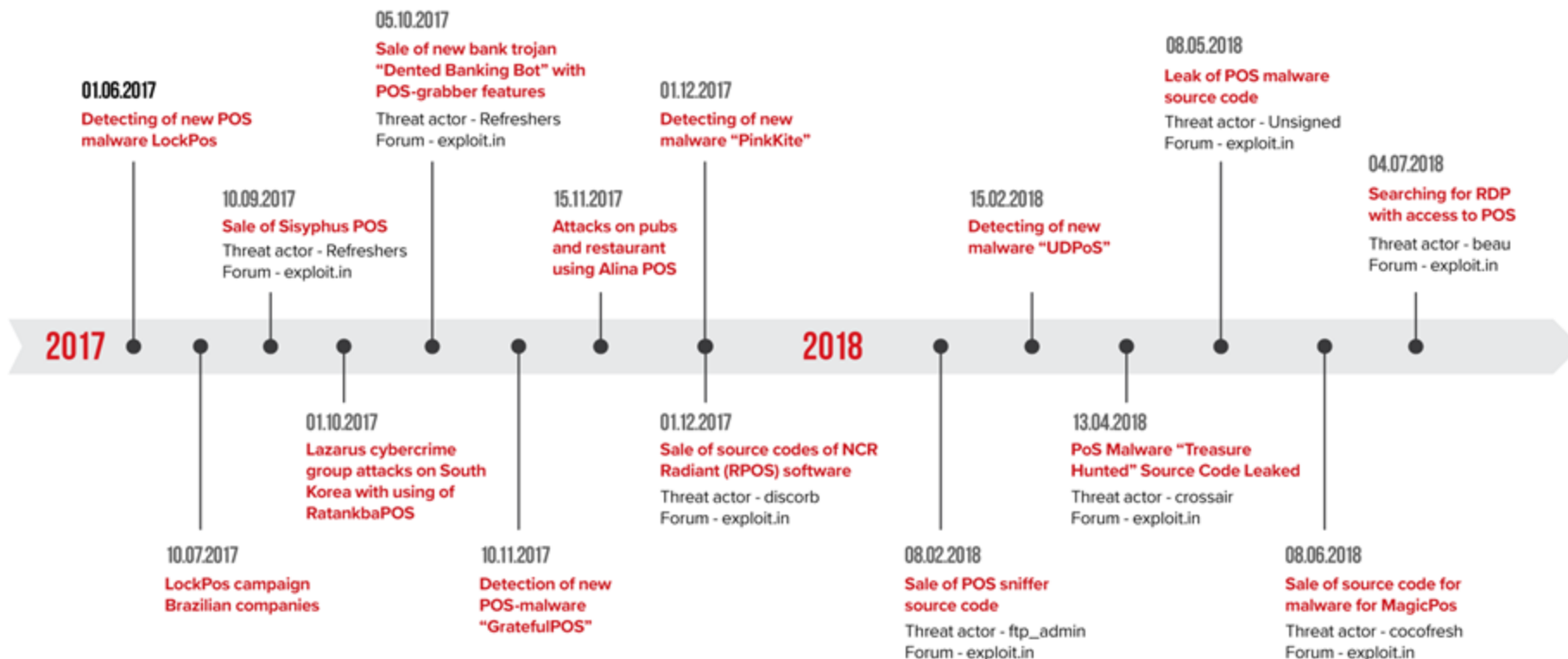


CARDING

	Text data	Dumps	Total
Total number	10 218 489	16 927 777	27 146 266
Market volume	\$95 590 424	\$567 791 443	\$663 381 867
Lowest price	\$0.75	\$0.5	
Highest price	\$99.99	\$295	
Average price	\$9.35	\$33.54	
Median	\$8	\$25	

1.8 MLN CARDS WERE UPLOADED TO CARDSHOPS

- 62% of data sold is connected to card data dumps
- POS Trojans are the main method of getting the dumps
- Text data accounts for just 17% of all card-related market.





PREDICTIONS



ROUTERS ARE A POINT OF GROWTH

- Wi-Fi in restaurants will become the main method of POS terminal penetration and infection.
- Forwarding to phishing by manipulating traffic at the router level.



ATM JACKPOTTING

- In various countries Cutlet is the main tool to attack ATMs with physical access.
- We should expect growth in the number of logical attacks following banks hacking. All groups have relevant Trojans in their armory now.



BANKING TROJANS

- Android Trojans will start to attack organizations through contextual advertising.
- Android will continue to replace PC Trojans.
- PC Trojan BackSwap and IcedID can become a significant threat for banks in the USA and Europe.



DAMAGE FOR BANK CUSTOMERS

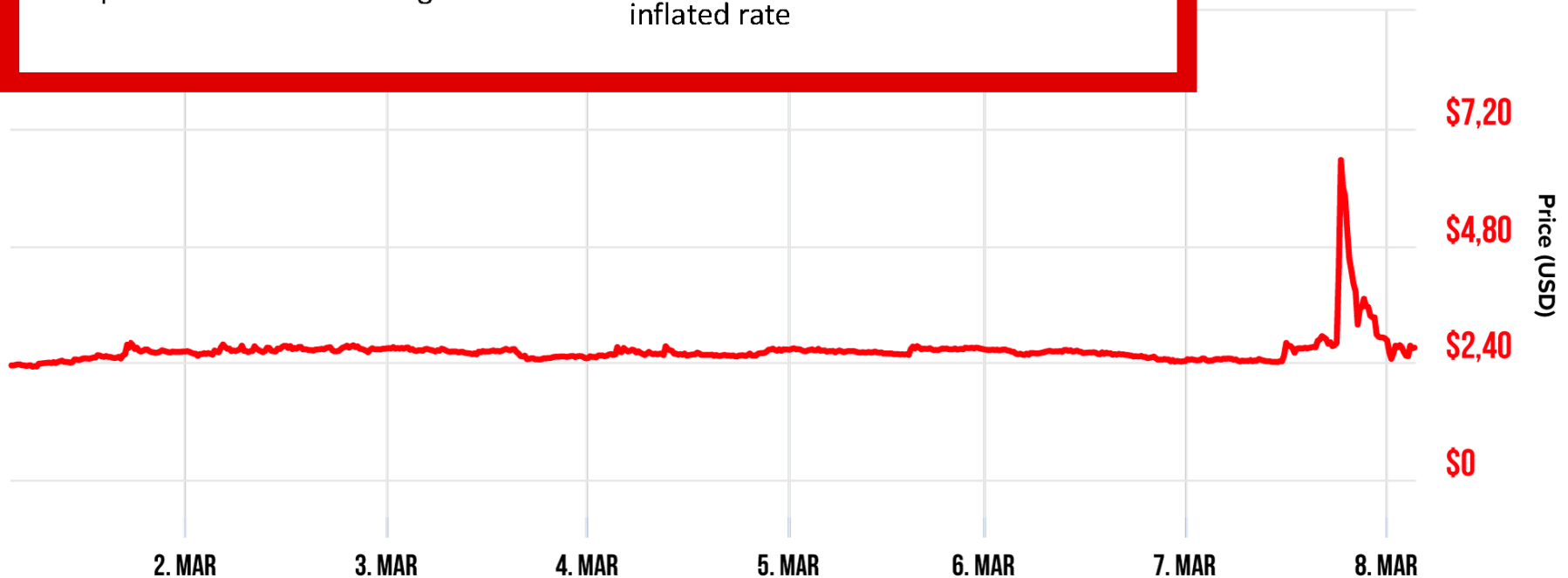
- There will be a reduction in all areas except for targeted attacks.
- Phishing will be the main source of damage.



THREATS FOR THE CRYPTOCURRENCY MARKET: MANIPULATION WITH THE CRYPTOCURRENCY EXCHANGE RATE

ATTACKERS' TACTICS

- Phishing website disguised as the Chinese exchange Binance
- Collection of logins and passwords of traders
- Generation of API keys to automate operations on the exchange
- In 2 minutes, generation of trader applications for the little-known cryptocurrency Viacoin
- In 30 minutes, Viacoin rate jumped by 143%
- Selling Viacoin via Bitcoin with the inflated rate





THREATS FOR THE CRYPTOCURRENCY MARKET: 51% ATTACK

Double-spending is considered to be the biggest threat to the system.

Having 51% of computing power, the attacker can create a stealthy alternative blockchain and use it to confirm an attacker's own transactions.

 **Chandler Guo**
@ChandlerGuo

I am Chandler Guo, a 51% attack on Ethereum Classic (ETC) is coming with my 98G hashrate powtopos.com
15:33 - 24 июл. 2016 г.



powtopos
pow to pos
powtopos.com

33 61 человек(а) говорят об этом

APRIL 4

VERGE

An attacker could mine \$1 million worth of cryptocurrency.

MAY 18

BITCOIN GOLD

An attacker could mine \$18 million worth of cryptocurrency.

MAY 22

VERGE

SuperNova reported that Verge was under 51% attack and all correct blocks are rejected.

JUNE 3

ZENCASH

An attacker could mine \$550,000 worth of cryptocurrency.

JUNE 6

LITECOIN CASH

Litecoin (LTC) fork also faced 51% attack.



THREATS FOR THE CRYPTOCURRENCY MARKET: TARGETED HACKING OF CRYPTO EXCHANGES

NUMBER OF THEFTS BECAME **5 TIMES LARGER**
COMPARED TO THE PREVIOUS YEAR

2016
**\$168
MLN**

NORTH KOREA IS THE MAIN THREAT

- 5 out of 10 thefts are believed to be connected to Lazarus
- Most exchanges which have become victims are from South Korea
- YouBit/Yapizon went bankrupt.

2017
\$877 MLN

61% of the total is
stolen from Coincheck

THIRD PARTY ATTRIBUTION FROM OPEN SOURCE

Date	Name of Project	Country	Criminal group	Stolen in cryptocurrency	Stolen in USD
Feb 2017	Bithumb	South Korea	Unknown	-	\$7 mln
Apr 2017	YouBit	South Korea	Unknown	-	\$5,6 mln
Apr 2017	Yapizon	South Korea	Lazarus	3,816 BTC	\$5,3 mln
Aug 2017	Ether Delta	-	Unknown	-	\$277 k
Aug 2017	OKEx	Hong Kong	Unknown	-	\$3 mln
Sep 2017	Coinis	South Korea	Lazarus	-	-
Dec 2017	YouBit	South Korea	Lazarus	17% of assets	-
Jan 2018	Coincheck	Japan	Lazarus	523 mln NEM	\$534 mln
Feb 2018	Bitgrail	Italy	Unknown	17 mln NANO	\$170 mln
Jun 2018	Bithumb	South Korea	Lazarus	-	\$32 mln
Jun 2018	Coinrail	South Korea	Unknown	11 types of cryptocurrency	\$37 mln
Jun 2018	Bancor	-	Unknown	-	\$23 mln
Sept 2018	Zaif	Japan	Unknown	-	\$60 mln
TOTAL					\$877 MLN



PREDICTIONS



REDUCTION OF MINING

- Cryptojacking boom is over.
- Trojans are no longer efficient for mining.



NEW ATTACKERS

- Silence, MoneyTaker, and Cobalt may conduct several successful targeted attacks on exchanges and the largest miners.



THE LARGEST MINERS

- They will become the main target of the pro-government attackers to control 51% of power and take over the cryptocurrency control.



ICO

- It is still the target for hackers.
- However, the number of attacks will decline.